ABSTRACT

A system and method for detecting a drone implanted by a vandal in a network connected host device such as a computer, and controlling the output of the drone. The system includes an inbound intrusion detection system (IDS), an outbound IDS, a blocker such as a firewall, an inbound trace log for storing a trace of inbound traffic to the protected device, an outbound trace log for storing a trace of outbound traffic from the protected device, and a correlator. When the outbound IDS detects outbound distributed denial of service (DDoS) traffic, the outbound IDS instructs the blocker to block the outbound DDoS traffic. The correlator then recalls the outbound trace log and the inbound trace log, correlates the logs, and deduces the source ID of a message responsible for triggering the drone. The correlator then instructs the blocker to block incoming messages that bear the source ID.